SECURITY DOMAIN MINUTES

Date: November 8, 2002

Attendees

- Steve Adams
- Dustin Bieghler
- Dawna Cape
- Curt Christian
- Stephen Derendinger
- Gail Keisker
- Barb Kiso

- Doug Less
- Bob Meinhardt
- Lora Mellies
- Mike Miller
- Gail Morris
- R.D. Porter
- Pete Wieberg

Agenda Discussion

Detailed notes available

Introductions

All participants gave a brief introduction of themselves, previous experience, and thoughts on the charge of the Security Domain. Some of those ideas are listed below:

- Populate architecture
- Statewide applicable policies and procedures, guidelines, standards, …
- Ease future implementations
- Utilize expertise to ensure all areas covered
- Planning process
- Vitality process – keep things current
- Statewide integration, interoperability, direction, …

Of particular concern was ensuring statewide applicability and adaptability of the architecture elements in order to benefit both agencies' unique needs, as well as the collective whole.

■ MAEA Program Review

   ▪ Slide comments:
      ❑ It was suggested that the Security Domain Mission should be enhanced to include reference to trust and interoperability.
      ❑ Familiarity with the "blue box" concept (e.g., how architecture elements are related) is important in understanding context for domain decisions.

   ▪ The directive from the B. Meinhardt is for the domain committee to determine what can be produced, and subsequently delivered, that will provide the most value to the agencies.

■ Roles and Responsibilities

   ▪ Domain Committee Chairperson
      ❑ Although governance model indicated the chairperson was to be chosen by the ARC, the group was given the opportunity to elect their own leader
      ❑ Dustin Bieghler was elected as the initial Domain Committee Chairperson, with Lora Mellies volunteering to serve as Vice-Chair
      ❑ Mr. Meinhardt offered OIT's support and availability for legwork

   ▪ NSR is responsible for the following items:
      ❑ Meeting facilitator and scribe roles
      ❑ Laying out process and identifying lessons learned
      ❑ Delivering facilitation guide

■ Security Domain and Disciplines

   ▪ The domain definition was modified to provide a concise statement utilizing three globally accepted protection requirements.

      The Security domain defines the technologies, standards, and guidelines necessary to ensure the confidentiality, integrity and availability of the information and technology assets of the State of Missouri.

   ▪ After considerable deliberation and reviewing information provided by Lora, the group decided to utilize information from NIST for the preliminary structure of security components. Following are a few of the benefits:
      ❑ NIST is utilized among numerous organizations (federal and state) and provides a common "language" for discussion
      ❑ Utilizing an existing, researched framework reduces analysis and development time
      ❑ Standards developed by NIST can be used as a starting point and /or as supporting documentation

- The initial disciplines were replaced in order to align the Security Domain structure with NIST standards.
  - Management Controls
  - Operational Controls
  - Technical Controls

■ Security Domain Subject Areas

- The initial subject areas were replaced with the seventeen topic areas identified for the three NIST classes previously noted.

■ Subject Area Homework

- The initial 17 subject areas were reduced to 8 for an initial target group. They were identified based on value to the enterprise and level of effort required.

- Committee members were tasked with completing the Subject Area Worksheet for a designated subject area.
  - Personnel Security – Lora
  - Physical Security – Steve
  - Hardware & Systems Software – Curt
  - Data Integrity – Pete
  - Security Awareness, Training & Education – Gail M
  - Incident Response Capability – R.D.
  - Identification and Authentication – Gail K.
  - Logical Access Controls -- Dustin

Action Items

■ Committee:
  - Complete Subject Area Worksheet and send to Dawna Cape at dcape@roseint.com. **November 18, 2002**
  - Review MAEA technology scan processes. **November 21, 2002**
  - Identify potential "deliverables" for agencies. **November 21, 2002**

■ D. Cape: Distribute soft copy of Subject Area Worksheet, web resource list, and committee contact list to committee members. **November 8, 2002**